UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,109	12/20/2001	Donald P. Matthews JR.	2875.0660001	7508

26111 7590 10/15/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/026,109	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24 and 29-31* is/are rejected.

7)☒ Claim(s) *25-28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 24-31 are pending.

2. Response filed 09/10/2007 has been received and fully considered.

Claim Objections

3. Claim 31 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Each of the limitations in the body (the four stages) of the claim are the same as those in independent claim 24. Furthermore, the preamble states the values are shuffled, however, the third and fourth stages perform this shuffling in both claim 31 and claim 24.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at

> the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 24, 29, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matthews, Jr. (US 6549622) in view of Parker et al. (US 20020186839).

As per claims 24 and 31, Matthews, Jr. discloses a cryptographic accelerator for performing an RC4 stream cipher, comprising: a multi-ported memory having at least three read ports and at least two write ports (see figure 6 numerals 604 and 606 where each has dual ports and therefore has at least 4 or each read and write ports); and a cryptographic core having a four-stage pipeline, wherein during a key generation process the cryptographic core is configured to: in a first stage, increment the value of a first memory address location (see column 1 lines 60-61, column 12 lines 60-61, figure 9 numeral 902), in a second stage, read data stored at a previous first memory address location and calculate a value of a second memory address location (see column 1 lines 62-64, column 12 lines 61-62, figure 9 numeral 904), in a third stage, read data stored at a previous second memory address location, calculate a value of a third memory address location, and write data stored at a previous first memory address location to the previous second memory address location (see column 1 lines 64-67, column 12

lines 62-64, figure 9 numeral 906), and in a fourth stage, read data stored at a previous third memory address location and write data stored at the previous second memory address location to a previous first memory address location (see column 1 lines 60-67, column 12 lines 62-64 and figure 9 numeral 908).

Matthews, Jr. fails to explicitly disclose after three initialization clock cycles, a byte of a key stream is generated in the fourth stage.

However, Parker et al. teaches such an initialization method (see paragraphs 46-49).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to initialize the system of Matthews, Jr. after three clock cycles.

Motivation to do so would have been that it is faster than the typical six cycles the initialization (see Parker et al. paragraph 46).

As per claim 29, the modified Matthews, Jr. and Parker et al. system discloses the multi-ported memory is a register (see Parker et al. figure 1).

6. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Matthews, Jr. and Parker et al. system as applied to claim 29 above, and further in view of Batcher (US 6873707).

As per claim 30, the modified Matthews, Jr. and Parker et al. System fails to disclose the register is a flip-flop based register.

However, Batcher teaches such a flip-flop type register (see column 9 lines 32-36).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the register of the modified Matthews, Jr. and Parker et al. system to be a flip-flop based register.

Motivation to do so would have been that there is very little slack in setup timing (see Batcher column 9 lines 32-36).

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or

provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 24, 29, and 31 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 9, 11, and 15 of U.S. Patent No. 6549622 in view of Parker et al. As per claims 24 and 31 the patented claims fail to explicitly disclose after three initialization clock cycles, a byte of a key stream is generated in the fourth stage and the address shifting.

However, Parker et al. teaches such an initialization method (see paragraphs 46-49) and the address shifting with hardware (see figure 2).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to initialize the system of the patented claims after three clock cycles.

Motivation to do so would have been that it is faster than the typical six cycles the initialization (see Parker et al. paragraph 46).

As per claim 29, the modified claims and Parker et al. system discloses the multi-ported memory is a register (see Parker et al. figure 1).

Allowable Subject Matter

8. Claims 25-28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. The following is a statement of reasons for the indication of allowable subject matter: Claim 25 (from which claims 26-28 depend) further details the initialization method generally described in claim 24. Specifically, the first three stages are implemented with an iteration of the value of the first memory address location (i). The prior art teaches incrementing the this value at the first step and the third step (see Matthews, Jr. claim 11 step (e) where (a) corresponds to the first stage, (b) and (c) correspond to the second stage, (d) and (e) correspond to the third stages, and (f) and (g) correspond to the fourth stage), but fails to teach incrementing the value at the second stage, nor is any motivation given as to why one would perform this additional incrementing step. Claims 26-28

depend (directly or indirectly) from claim 25 and are allowable for the same rationale.

Response to Arguments

10. Applicant's arguments filed 09/10/2007 have been fully considered but they are not persuasive. Applicant argues that claim 31 is a proper dependent claim; the claimed references fail to disclose a byte of the key stream is generated in each subsequent clock cycle after a set of initialization clock cycles; and the double patenting rejection is improper.

With respect to Applicant's argument that claim 31 is a proper dependent claim, claim 31 contains the same stages as those being performed in claim 24, from which it depends. While the core is "further configured to shuffle values" the core of claim 24 already is configured to do this because the steps result in another key stream byte being generated, so the stages are clearly repeated for each byte being generated.

With respect to Applicant's argument that the claimed references fail to disclose a byte of the key stream is generated in each subsequent clock cycle after a set of initialization clock cycles, the combined references teach each of the limitations, where pipeline is given its broadest reasonable interpretation as "A category of techniques that

provide simultaneous, or parallel, processing within the computer." (from Answers.com) and Parker teaches performing operations in parallel in paragraphs 46-49. Therefore Parker teaches a pipelined cryptographic processor. Since all the process steps are recited in the cited references the intended result (i.e. the last wherein clause) would fall naturally from the references. Furthermore, the courts have noted (quoting Minton v. Nat'l Ass'n of Securities Dealers, Inc., 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited." (See also MPEP 2111.04)

Applicant's argument that the double patenting is improper is moot in view of the above response.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened

statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER